



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/328,726	10/26/1998	THOMAS COLLINS	2026-25(PT-TA 410(Cont1))	7212
7590	11/03/2004		EXAMINER	SEAL, JAMES
HEWLETT-PACKARD COMPANY Attn: Bill Streeter Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			ART UNIT	PAPER NUMBER
			2135	DATE MAILED: 11/03/2004

34

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/328,726	COLLINS ET AL.
	Examiner	Art Unit
	James Seal	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 21 June 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 17-66, 73-122 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 17-66 and 73-122 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 21 April 2004.
2. Claims 17-66 and 73-122 are pending.

Claim Objections

Claim 113 is objected to because of the following informalities: Line 6, p₁, p₂, ..., P_k should be p₁, p₂, ..., p_k. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest.

10. As per claim 17, the limitation of a cryptographic system which breaks messages into blocks M of size $0 \leq M \leq n$ where n is a modulus of an RSA encryption algorithm

$$C \equiv M^e \pmod{n}$$

$$M \equiv C^d \pmod{n}$$

$$ed \equiv 1 \pmod{\lambda(n)}$$

Art Unit: 2135

the latter would imply

$$d \equiv e^{-1} \pmod{\lambda(n)}$$

such that $n \in \mathbb{Z}$ with prime factorization

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$$

$$\lambda(n) = \text{lcm} \{ \lambda(p_1^{e_1}) \lambda(p_2^{e_2}) \lambda(p_3^{e_3}) \dots \lambda(p_k^{e_k}) \}$$

for which if $e_i > 2$

$$\lambda(p_i^{e_i}) = \phi(p_i^{e_i})$$

is the Euler totient and if $e_i = 1$

$$\phi(p_i) = p_i - 1$$

with e relatively primed to $(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)$ which would imply

$$d \equiv e^{-1} \pmod{(p_1-1)(p_2-1)(p_3-1)\dots(p_k-1)}$$

Is disclosed in Lidl page 289, lines 3, 5-6, bottom page 290, page 291 lines 3-7, page 293 problem 11. Lidl does not disclose the use of the Chinese Remainder Theorem (CRT) with respect to the problem at hand; however, by way of example, Lidl does teach application of his teachings to the special case of where the prime factors are distinct $p_1 = p$ and $p_2 = q$, that is, $e_1 = e_2 = 1$.

Quisquater teaches reduction RSA (two prime factors p and q) calculation to a simultaneous system of modular congruences

$$C_1 \equiv C \pmod{p_1}$$

$$C_2 \equiv C \pmod{p_2}$$

$$M_1 \equiv C_1^{d_1} \pmod{p_1}$$

$$M_2 \equiv C_2^{d_2} \pmod{p_1}$$

$$d_1 \equiv d \pmod{(p_1-1)}$$

$$d_2 \equiv d \pmod{(p_2-1)}$$

Solving for the results for M_1 and M_2 and combining the sub-task to produce the receive message M . Reducing the calculations to simultaneous sub-task allows Quisquater to carry out the calculations much faster as p_1 and p_2 , d_1 , d_2 , M_1 , M_2 and C_1 , C_2 are much smaller in terms of the number of bits (see page 906 lines 3-8, 31-39, 55-60). Further such subtasks may be applied in parallel (see parallel below (1), "moreover the two computations may be done in parallel" and figure 1, for example the exponentiation modules $x^2 \bmod p$ and $x^2 \bmod q$ which calculate different subtasks at the same time. Thus one of ordinary skill in the art would recognize the speed and savings in computational resources which could be derived from using the teachings of Quisquater and would be strongly motivated to apply these teaching to Lidl algorithm. Lidl pages 515-517 also teaches the generalization of the above process for the case of k factors.

Lidl is silent on the choice of the e_i 's, as he is seeking to generalize the RSA system to its fullest. The RSA paper teaches both *randomness* and *distinctness* are important in the selection of primes for the two prime factors p and q scheme that they propose (see Rivest et. al. page 6, line 34 ;page 9, lines 2-3, and line 26-27) in order to maximize security. If the size of the modulus n is restricted to 200 digits, then maximum security is attained by taking by choose p and q differing by a few digits (*distinctness*) and chosen at random. Thus if randomness and distinctness is not applied to multifactor scheme, one losses the randomness that is there are a lot fewer ways to choose a two hundred digit number of the form $p^2 q$ as opposed to pqr and hence a loss of security. Thus one of ordinary skill in the art would recognize in order to maximize security one

Art Unit: 2135

must increase the number of possible choices which implies distinctness of all factors that is $e_1 = e_2 = e_3 = \dots = e_k$ in the teaching of Lidl. Thus one of ordinary skill of the art would have been motivated to combine the general teachings of extent the teaching of Rivest using the teaching of Lidl and with the speed enhancements of Quisquater to obtain high security which is fast and could run in order to run RSA and digital signature algorithms on devices with limited computational resources such as CD ROM's, smartcards, secure net browser, cellphones, etc. Claim 17 is rejected.

3. Claim 18-66 and 73-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et. al. The Chinese Remainder Theorem, World Scientific.

4. As per claim 18-21, the details of a recursive (iterative) algorithm is given page 23. Note the relabelling of the dummy indices and the use of the extended Euclidian algorithm $u_i M_i + v_i m_i = 1$ to provide the inverse u_i or w^{-1} , modulo m_k or p_i in 2.8 of the product M_k corresponding to applicant's w_i . Claims 18-21 are rejected.

5. Claims 22-26 are a system implementation of claims 17-21 and are rejected in view of the same prior art of record.

6. In claim 17, the limitation of the decomposition into subtasks performed simultaneously, of the RSA decryption equation was applied without any corresponding

Art Unit: 2135

application of the same technique to the encryption part of the encryption system. The limitations of claims 27 are directed to the same decomposition into subtasks to be performed simultaneously. One of ordinary skill in the art recognizing the same benefits may be had by applying the same mathematics to the encryption area would have been motivated to apply it to the encryption part of the cryptosystem to gain the same benefits. Claim 27 is rejected.

7. As per claims 28-31, expand upon the CRT algorithm applied to this aspect of the encryption and would be rejected on the same group as claims 18-21. Claims 28-31 are rejected.

8. Claims 32-36 are a system implementation of claims 27-31 and are rejected in view of the same prior art of record. Claims 27-31 are rejected.

9. Claims 37-41 and 44 recite a method for decoding corresponding to the method of encoding claims of 17-22 and are rejected in view of the same prior art (all references disclosed both an encoding and decoding scheme). Claim 37-41 and 44 are rejected.

10. As per claims 42-43, and 45-46, the limitation of a cryptographic system for decoding implementing method of claims 37-41, and 44 is rejected in view of the same prior art of record. Claims 42-41 and 44 are rejected.

11. As per claim 47-51, the limitation for a method of generating digital signature is disclosed by Rivest (see pages 4-6) for two prime factors. Using the Lidl/Quisquater/Ding scheme, one of ordinary skill in the art would have also been motivated to apply the same techniques to digital signature to increase speed, conserve computational resources which are important credit card transactions, and digital rights management. Claims 47-51 are rejected.

Art Unit: 2135

12. Claims 52-56 are a system implementation for the generating method recited in claims 47-52 and is rejected in view of the same prior art of record. Claims 52-56

13. As per claims 57-61, the limitations of a process for verifying digital signatures, recited in the method claims 47-52 is disclosed by Rivest (page 5). Claims 57-61 are rejected.

14. Claims 62-66, recite a system for generating and validating digital signatures corresponding to method claims 47-51 and 57-61 and are rejected in view of the same prior art of record.

15. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 recites the limitation of a plurality of exponentiator units operating substantially simultaneously and performing subtasks are disclosed by Figure 1 Quisquater. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 are rejected.

16. Claims 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 recite the limitation that each distinct random prime factor has the same number of bits is disclosed in Quisquater page 906 second column under figure 1.

17. Claims 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest, Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem and further in view of Knuth, The Art of Computer Programming vol 2 page 179.

Art Unit: 2135

18. As per claim 17, the limitation of a method for processing messages in a communication system with RSA public key encryption an alternative embodiment of the present invention (see Figure 6, Abstract line 1 of Column 4, lines 15 through Column 5, lines 11, RSA), such that three or more primes $p_1, p_2, p_3, \dots, p_k$ are generated, such that $k > 2$ (Column 13, lines 30-31) then using the present invention (Column 13, line 29) provided and e relatively prime to $\phi(n)$ (Column 13, lines 42-44), $\phi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1) \dots (p_k - 1)$, that is, relatively prime to $(p_1 - 1)(p_2 - 1)(p_3 - 1) \dots (p_k - 1)$ and generating from the product of these primes and integer n which will be the resulting modulus n (Column 13, line 30-31, line 34) using the provided e and n together with a message M where $0 \leq M \leq n-1$ (Column 4, line 26), and the RSA encryption algorithm $C \equiv M^e \pmod{n}$ (Column 4, line 59, RSA) to generate a cipher text C, decrypting C at the intended recipient (Column 6, 29-31) having available to it. RSA suggest the CRT but is silent on the details. Quisquater provides the details and motivations (see discussion in claim 17 above) for the implementation for two parameters.

19. The RSA paper teaches both *randomness* and *distinctness* are important in the selection of primes for the two prime factors p and q scheme that they propose (see Rivest et. al. page 6, line 34 ;page 9, lines 2-3, and line 26-27) in order to maximize security. If the size of the modulus n is restricted to 200 digits, then maximum security is attained by taking by choose p and q differing by a few digits (*distinctness*) and chosen at random. Thus if randomness and distinctness is not applied to multifactor scheme, one losses the randomness that is there are a lot fewer ways to choose a two hundred digit number of the form $p^2 q$ as opposed to pqr and hence a loss of security. Thus one of ordinary skill in the art would recognize in order to maximize security one

Art Unit: 2135

must increase the number of possible choices which implies distinctness of all factors that is $e_1 = e_2 = e_3 = \dots = e_k$. Thus one of ordinary skill of the art would have been motivated to combine the general teachings of Lidl with the additional speed enhancements of Quisquater and finally the security teachings of the original RSA paper to obtain a security system which is fast and could run on devices with limited computational resources such as CD ROM's, smartcards, secure net browsers, etc.

20. RSA patent recites a different embodiment (Column 13, lines 30-31) in which the modulus n is a product of three or more primes (not necessarily distinct primes). RSA further goes on to state that decoding may be performed modulo each of the prime factors of n (thus breaking the calculations into a series of subtasks involving the factors of n and not n) and then combining the results using "Chinese remaindering" (that is the Chinese remainder theorem henceforth CRT). However, only in the case of distinct primes can the decoding problem be performed using the CRT. In the case of non-distinct primes one would need in addition Hensel's Lemma (or a generalization by Hensel of p-adics, see Knuth vol 2, page 179). Thus it is clear that the RSA patent is referring to the case of distinct primes. Claim 1 is rejected.

21. Claim 18-66 and 73-122 rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) henceforth RSA, and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim

Art Unit: 2135

17 above, and further in view of Ding et. al. The Chinese Remainder Theorem, World Scientific.

22. As per claim 18-21, the details of a recursive (iterative) algorithm is given page

23. Note the relabelling of the dummy indices and the use of the extended Euclidian algorithm $u_i M_i + v_i m_i = 1$ to provide the inverse u_i or w^{-1}_i modulo m_k or p_i in 2.8 of the product M_k corresponding to applicant's w_i . Claims 18-21 are rejected.

23. Claims 22-26 are a system implementation of claims 17-21 and are rejected in view of the same prior art of record.

24. In claim 17, the limitation of the decomposition into subtasks performed simultaneously, of the RSA decryption equation was applied without any corresponding application of the same technique to the encryption part of the encryption system. The limitations of claims 27 are directed to the same decomposition into subtasks to be performed simultaneously. One of ordinary skill in the art recognizing the same benefits may be had by applying the same mathematics to the encryption area would have been motivated to apply it to the encryption part of the cryptosystem to gain the same benefits. Claim 27 is rejected.

25. As per claims 28-31, expand upon the CRT algorithm applied to this aspect of the encryption and would be rejected on the same group as claims 18-21. Claims 28-31 are rejected.

26. Claims 32-36 are a system implementation of claims 27-31 and are rejected in view of the same prior art of record. Claims 27-31 are rejected.

Art Unit: 2135

27. Claims 37-41 and 44 recite a method for decoding corresponding to the method of encoding claims of 17-22 and are rejected in view of the same prior art (all references disclosed both an encoding and decoding scheme). Claim 37-41 and 44 are rejected.

28. As per claims 42-43, and 45-46, the limitation of a cryptographic system for decoding implementing method of claims 37-41, and 44 is rejected in view of the same prior art of record. Claims 42-41 and 44 are rejected.

29. As per claim 47-51, the limitation for a method of generating digital signature is disclosed by Rivest (see pages 4-6) for two prime factors. Using the Lidl/Quisquater/Ding scheme, one of ordinary skill in the art would have also been motivated to apply the same techniques to digital signature to increase speed, conserve computational resources which are important credit card transactions, and digital rights management. Claims 47-51 are rejected.

30. Claims 52-56 are a system implementation for the generating method recited in claims 47-52 and is rejected in view of the same prior art of record. Claims 52-56

31. As per claims 57-61, the limitations of a process for verifying digital signatures, recited in the method claims 47-52 is disclosed by Rivest (page 5). Claims 57-61 are rejected.

32. Claims 62-66, recite a system for generating and validating digital signatures corresponding to method claims 47-51 and 57-61 and are rejected in view of the same prior art of record.

33. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 recites the limitation of a plurality of exponentiator units operating substantially simultaneously and performing subtasks are

Art Unit: 2135

disclosed by Figure 1 Quisquater. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 are rejected.

34. Claims 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 recite the limitation that each distinct random prime factor has the same number of bits is disclosed in Quisquater page 906 second column under figure 1.

35. With regards to claims 93-112, these are depend in pairs on pre-existing claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 pair-wise and respectively, that is 93-94 are dependent on 17, 95-96 are dependent on 22 and so forth. The claimed limitation of claim 93, 95, ... is that the a plurality of k subtask are performed in parallel. Lidl suggest the generalization to k distinct primes. Rivest paper suggest primes should be choosen distinct and random and their reasoning would generalize to k distinct primes. Quisquater and Courveur disclose the use of parallel calculation of RSA in the case of two primes for the purpose of speeding up calculations and their reasoning would also apply to k distinct primes as the CRT may also be generalized to the case of k distinct primes. Thus one of ordinary skill in the art at the time the invention was made would have been motivated to to modify the teachings of Lidl with those of Quisquater and Couveur as the use of parallelism well greatly speed up the calculations. Claims 93, 95, 97, 99, 101, 103, 105, 107, and 111, are rejected.

36. For 94, 96, 98, ... the limitation of combining with the CRT k distinct parallel calculations is taught by Ding. Thus one of ordinary skill in the art at the time the invention was made would have been motivated to to modify the teachings of Ding on the usage of the CRT and parallel to implement it in combination with the teachings of Lidl, Rivest, and

Art Unit: 2135

Quisquater and Couveur as the use of parallelism well greatly speed up the calculations.

Claims 94, 96, 98, 102, 104, 106, 108, 110, and 112 are rejected.

37.

38. Claim 17 are rejected under 35 U.S.C. 103(a) in view of Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996 and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest and Quisquater Fast Decipherment Algorithm for RSA Public-key Cryptosystem, 1982.

39. Nemo discloses the use of a three prime RSA (see section 3). Each prime p, q, r would contain the same number of bits (256 bits) and the modulus n would contain 768 bits. The system would provide digital signature, encryption, decryption, and self encryption (files, backup tapes and archives) and in section 4.2 provide secure signed routers for networks. Nemo's three prime RSA is faster because of the CRT(section 3.1). Although, Nemo's three prime RSA applies CRT to decryption section, still greater speed could be achieved by applying to both encryption/decryption. Further, Nemo could be extended to k distinct primes to make the algorithm faster, using the arguments in Quisquater. Such details are supplied by Quisquater.

40. The RSA paper teaches both *randomness* and *distinctness* are important in the selection of primes for the two prime factors p and q scheme that they propose (see Rivest et. al. page 6, line 34 ;page 9, lines 2-3, and line 26-27) in order to maximize security. If the size of the modulus n is restricted to 200 digits, then maximum security is attained by taking by choose p and q differing by a few digits (*distinctness*) and

Art Unit: 2135

chooseen at random. Thus if randomness and distinctness is not applied to multifactor scheme, one losses the randomness that is there are a lot fewer ways to choose a two hundred digit number of the form $p^2 q$ as opposed to pqr and hence a loss of security. Thus one of ordinary skill in the art would recognize in order to maximize security one must increase the number of possible choices which implies distinctness of all factors that is $e_1 = e_2 = e_3 = \dots = e_k$. Thus one of ordinary skill of the art would have been modivated to combine the general teachings of Lidl with the additional speed enhancements of Quisquater and finally the security teachings of the original RSA paper to obtain a security system which is fast and could run on devices with limited computational resources such as CD ROM's, smartcards, secure net browers, etc.

Claim 1 is rejected.

41. Claim 18-66 and 73-122, rejected under 35 U.S.C. 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996, and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et. al. The Chinese Remainder Theorem, World Scientific.

42. As per claim 18-21, the details of a recursive (iterative) algorithm is given page 23. Note the relabling of the dummy indices and the use of the extended Euclidian algorithm $u_i M_i + v_i m_i = 1$ to provide the inverse u_i or w^{-1}_i modulo m_k or p_i in 2.8 of the product M_k corresponding to applicant's w_i . Claims 18-21 are rejected.

Art Unit: 2135

43. Claims 22-26 are a system implementation of claims 17-21 and are rejected in view of the same prior art of record.

44. In claim 27, the limitation of the decomposition into subtasks performed simultaneously, of the RSA decryption equation was applied without any corresponding application of the same technique to the encryption part of the encryption system. The limitations of claims 27 are directed to the same decomposition into subtasks to be performed simultaneously. One of ordinary skill in the art recognizing the same benefits may be had by applying the same mathematics to the encryption area would have been motivated to apply it to the encryption part of the cryptosystem to gain the same benefits. Claim 27 is rejected.

45. As per claims 28-31, expand upon the CRT algorithm applied to this aspect of the encryption and would be rejected on the same group as claims 18-21. Claims 28-31 are rejected.

46. Claims 32-36 are a system implementation of claims 27-31 and are rejected in view of the same prior art of record. Claims 27-31 are rejected.

47. Claims 37-41 and 44 recite a method for decoding corresponding to the method of encoding claims of 17-22 and are rejected in view of the same prior art (all references disclosed both an encoding and decoding scheme). Claim 37-41 and 44 are rejected.

48. As per claims 42-43, and 45-46, the limitation of a cryptographic system for decoding implementing method of claims 37-41, and 44 is rejected in view of the same prior art of record. Claims 42-41 and 44 are rejected.

49. As per claim 47-51, the limitation for a method of generating digital signature is disclosed by Rivest (see pages 4-6) for two prime factors. Using the Lidl/Quisquater/Ding

Art Unit: 2135

scheme, one of ordinary skill in the art would have also been motivated to apply the same techniques to digital signature to increase speed, conserve computational resources which are important credit card transactions, and digital rights management. Claims 47-51 are rejected.

50. Claims 52-56 are a system implementation for the generating method recited in claims 47-52 and is rejected in view of the same prior art of record. Claims 52-56

51. As per claims 57-61, the limitations of a process for verifying digital signatures, recited in the method claims 47-52 is disclosed by Rivest (page 5). Claims 57-61 are rejected.

52. Claims 62-66, recite a system for generating and validating digital signatures corresponding to method claims 47-51 and 57-61 and are rejected in view of the same prior art of record.

53. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 recites the limitation of a plurality of exponentiator units operating substantially simultaneously and performing subtasks are disclosed by Figure 1 Quisquater. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 are rejected.

54. Claims 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 recite the limitation that each distinct random prime factor has the same number of bits is disclosed in Quisquater page 906 second column under figure 1.

55. As per claims 93-112, claims 93, 95, 97, 99, 101, 103, 105, 107, 109, and 111recite the limitation that a plurality of k sub-tasks are performed in parallel is taught by Quisquater and Couvreur. As noted in their paper "Fast Decipherment Algorithm For RSA Public-key Cryptosystem (the paragraph below equation (1)) "Moreover the two computations may be

Art Unit: 2135

done in parallel" thus teaching the CRT as a means of parallel processing. Claims 93, 95, 97, 99, 101, 103, 105, 107, 109, and 111 are rejected.

56. Claims 94, 96, 98, 100, 102, 104, 106, 108, 110, and 112 recite the further limitation wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT) is taught by Quisquater and Couvreur (see sentence above (1)). Claims 94, 96, 98, 100, 102, 104, 106, 108, 110, and 112 are rejected.

57. Claims 113-122, have the same limitations as 17, 22, 27, 32, 57, and 62 with the exception that the subtasks are performed in parallel and combined using the CRT. Lidl extends the method of Rivest to k distinct prime random chosen numbers, and Quisquater and Couvreur indicate the method of combining the results with two random distinct primes and Ding generalizes the results to k distinct random primes. One of ordinary skill in the art at the time the invention was made would have been motivated to have used have calculated using k parallel operation as this would provide speed due to the primes would be of less digits and the operations computed in parallel run much faster and then to combine the results of these k subtask with the CRT to obtain a final results

Response to Arguments

58. Applicant's arguments with respect to claim 17-66 and 73-122 have been considered but persuasive.

59. With regards to the admissibility of the Nemo paper "RSA Moduli Should Have 3 Prime Factors" dated August 1996:

Art Unit: 2135

Examiner argues that *Protein Foundation v. Brenner* does not apply to the Nemo paper since it is not a traditionally printed magazine. Examiner notes that the argument of choosing a later date than published is based on the inherent latency of the U.S. Post Office. Thus, arguing the applicability of *Protein Foundation v. Brenner* to the Nemo paper is equivalent to arguing the applicability of the attributes of the U.S. Post Office to an electronic publication. However, the Nemo paper was published electronically which assured a virtually instantaneous distribution, effectively bypassing the U.S. Post Office.

Additionally, MPEP 2128 (Section Titled: "Electronic Publications As Prior Art") states:

"Prior art disclosures on the Internet or on an on-line database are considered to be publicly available as of the date the item was publicly posted."

According to the copyleft date, the posting date is August 1996.

Applicant's assertion that the Nemo publication has not been published in such a manner that anyone who chose might avail themselves of the information it contains, is equivalent to stating that the Nemo copyleft date statement is in error.

Note that MPEP 2121.01 states that the test of applicability is whether an enabling disclosure is provided, which is the case regarding the Nemo paper. Furthermore, Examiner is required to presume that a reference's attributes are accurate and enabled in its entirety, unless evidence to the contrary is presented. However, existence of Applicant's specification provides evidence that the Nemo reference is accurate. As a result, Examiner has no reason to assume that the Nemo reference is accurate in all aspects, except for the copyleft date. Thus, unless Applicant can provide evidence that the Nemo article's copyleft date is in error or otherwise materially misstated, Examiner must admit the August 1996 date.

Examiner reminds Applicant that Applicant has a duty of disclosure and full candor (37 CFR 1.56 and MPEP 2000). Examiner notes that the Nemo paper in question, was provided under Applicant's IDS. However, Applicant's IDS is silent as to the source of the Nemo paper, be it from a magazine, from a web site, or otherwise. 37 CFR 1.98 states:

"(5) Each publication listed in an information disclosure statement must be identified by publisher, author (if any), title, relevant pages of the publication, date, and place of publication."

If Applicant is in this possession of information that would properly invalidate the August 1996 date for the Nemo paper, Examiner directs Applicant to provide this information forthwith.

Finally, Examiner notes that the Nemo paper discloses a mathematical and universal truth, specifically, RSA moduli should have three prime factors. MPEP 2124 states:

"In Some Circumstances a Factual Reference Need Not Antedate the Filing Date.

In certain circumstances, references cited to show a universal fact need not be available as prior art before applicant's filing date. *In re Wilson*, 311 F.2d 266, 135 USPQ 442 (CCPA 1962). Such facts include the characteristics and properties of a material or a scientific truism. Some specific examples in which later publications showing factual evidence can be cited include situations where the facts shown in the reference are evidence "that, as of an application 's filing date, undue experimentation would have been required..."

Since the Nemo paper discloses a mathematical and universal truth, even if Applicant were to swear behind the August 1996 date, the Nemo paper would still be admissible as prior art.

60. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

61. Applicant argues that Lidl teaches absolutely nothing with respect to a desire to improve speed or save computation resources. With regards to Lidl, the reference was used to lay the mathematical foundations of multiprime RSA and to indicate that a knowledge of this art was available to those of ordinary skill in the art as far back as 1984, twelve years before the applicants submitted their invention in 1996. With regards to Lidl teachings, it would appear that the applicants would agree with the examiner that multiprime RSA was not new or original to their invention as they state

that speed and conservation of resources not the multiprime RSA as taught in Lidl is what they consider important (see statement at the top of the second page of applicant's response in the remarks sections).

Quisquater disclose methods for speeding up RSA using parallel processing, made possible by the CRT decomposition (see Figure 1, sentence above equation (1) and next to the last line in paragraph under equation (1)), the recognition that performing computations with smaller rather than faster (see paragraph under equation (1); "the quantities p, q, c₁, c₂, d₁, d₂ are now about 300 bits long" as opposed to the ordinary RSA system in which the quantities such as "d would be about 500 or 600 bits long" and would further imply that storage of such quantities would require less memory and thus conservation of resources) and the elimination of any divisions in the computation (sentence above figure 1), application of these methods would increase the computational speed by a factor of 4 to 8 (Column 1, second paragraph). Thus one of ordinary skill in the art at the time the invention were made, would have recognized that by splitting n into multiple primes, that is the number of prime factors of n, would greatly increase the speed of a multi prime RSA. In the case of a 3 prime RSA, that would mean we would be performing computations on 200 bit number rather than 600 bit numbers and with 6 prime RSA 100 bits rather than 600 bit numbers. This would be in addition to the parallelism offered by the CRT would further make the speed of processing faster due to the simultaneous rather than sequential processing. Further Lidl teaches the extension of the CRT to r simultaneous congruences (see 515-516) thus making the art available for the r prime case.

The combination Lidl/Quisquater is silent on the selection of random and distinct prime factors. Rivest teaches both random selection of prime factors of n as well as distinctness of the primes(see Rivest 6, line 34; page 9, lines 2-3 and 26-27) in order to maximize security. If one considers making p and q, that is $p = q$, the same, and hunt for primes in the interval $N_1 \leq p \leq N_2$, then the number of products of the form $n = p^2$ in the interval is smaller than of the form $n = pq$, this would mean that a brute force attack over the interval would be more successive over those of the form $n = p^2$ than $n = pq$. This would imply that the former is less secure. Thus one of ordinary skill in the art at the time that the invention was made, would have been motivated to have combined the teaching of the Lidl/Quisquater system with the teaching of Rivest (random distinct primes) as it would provide greater security for the system. This is further amplified in examiner last action see pages 4 and 5.

62. With regards to claims 18-66 the applicant argues that the addition of Ding to the combination Lidl/quisquater/Rivest is attacking the references separately for a rejection which is based on a combination of references. The Ding supplies the details of a recursive algorithm which those in the art would have needed in order to implement the Lidl/quisquater/Rivest combination.

63. In response to applicant's argument that the examiner has combined an excessive number of references, reliance on a large number of references in a rejection does not, without more, weigh against the obviousness of the claimed invention. See *In re Gorman*, 933 F.2d 982, 18 USPQ2d 1885 (Fed. Cir. 1991).

Art Unit: 2135

64. With regards to the RSA/Revest/Quisquater/Knuth rejection, applicant implies that the number of references is excessive, that is four. The examiner would disagree. With the amount of mathematical details and corresponding limitations, four references is probably concise. The reference by Knuth, *The art of Computer Programming*, Vol. 2, page 179 is a well known reference for computational methods and was used to expand on what the prior art RSA, Rivest, and Quisquater in particular how the algorithms are applied in these references, that is fill in the details. RSA and Rivest represent the RSA patent and the journal article of the same. While they are not identical they are authored by the same authors and thus are used to get a better understanding of their invention.

65. With regards to RSA/Quisquater/Rivest/Ding rejection, applicant implies that the number of references is excessive, that is four. Again the examiner disagrees for the same reason as cited above. The RSA and Rivest references, in particular, describe the same invention of the same inventors and though they are not identical they describe the same invention from different viewpoints.

66. With regards to the combinations involving the Nemo reference see above.

67. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a

Art Unit: 2135

reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

68. With regards to the obviousness of the combinations, the examiner notes that in all of cases that the motivation to combine, is connected with making the original invention suggest in the RSA patent and the Rivest paper faster and more efficient without compromising its security. As pointed out by Quisquater and the other art one is limiting to several techniques, either to decrease the number of time consuming operations such as divisions, make use of techniques that can be possessed in parallel rather than sequentially or to decrease the size of the numbers (i.e. the number of digits) used in the computation, without decreasing the overall security of the system. The CRT provides part of the answer, in that it makes for parallel operations or to decrease the size of the primes use in the computation. The RSA, paper, the Lidl paper and the Nemo papers suggest that in order to do this one must increasing the number of prime factors in n while maintaining its size. The motivation is increased speed without compromising the security. The details of the motivations are slightly different depending on which art is applied (see previous Action), but the motivation in all cases is the same.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



James Seal
Examiner AU 2135
24 July 2004